Edith Cowan University
Strategic & Governance Services Centre

Critical Incident and Business Continuity Management Guidelines

Version	1.0
Relevance to	ECU Staff
Responsible staff	Chief Risk Officer
Responsible Office	Strategic and Governance Services Centre
Date introduced	April 2021
Date(s) modified	
Next scheduled review date	February 2024
Related University documents	Policy PL202: Critical Incident and Business Continuity Management Policy PL201: Integrated Risk Management
Related legislation and Standards	AS/NZ ISO 22301:2019: Business continuity management systems

Table of Contents

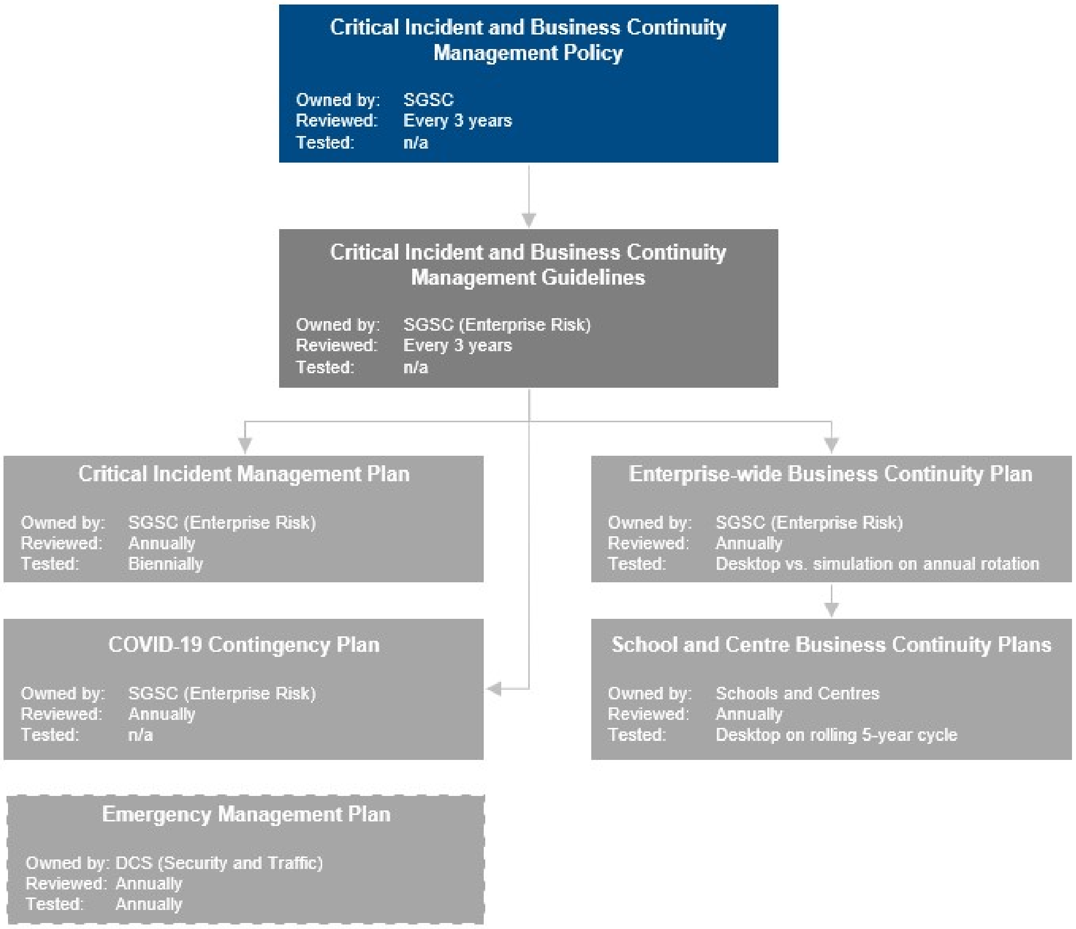
1. Purpose and scope

The purpose of the University's Critical Incident and Business Continuity Management ("CIBCM") framework is to provide a coordinated response to dealing with, and continuing business operations during a major or critical incident.

The Critical Incident and Business Continuity Management Guidelines ("the Guidelines") exist to support the University's CIBCM Policy and provide a consistent approach to responding to a major or critical incident.

Figure 1 below provides an overview of the University's CIBCM document framework:

Figure 1: CIBCM framework overview



Critical Incident and Business Continuity Management Policy

Owned by: SGSC
Reviewed: Every 3 years
Tested: n/a

Critical Incident and Business Continuity Management Guidelines

Owned by: SGSC (Enterprise Risk)
Reviewed: Every 3 years
Tested: n/a

Critical Incident Management Plan

Owned by: SGSC (Enterprise Risk)
Reviewed: Annually
Tested: Biennially

Enterprise-wide Business Continuity Plan

Owned by: SGSC (Enterprise Risk)
Reviewed: Annually
Tested: Desktop vs. simulation on annual rotation

COVID-19 Contingency Plan

Owned by: SGSC (Enterprise Risk)
Reviewed: Annually
Tested: n/a

School and Centre Business Continuity Plans

Owned by: Schools and Centres
Reviewed: Annually
Tested: Desktop on rolling 5-year cycle

Emergency Management Plan

Owned by: DCS (Security and Traffic)
Reviewed: Annually
Tested: Annually

2. Critical Incident and Business Continuity Management framework

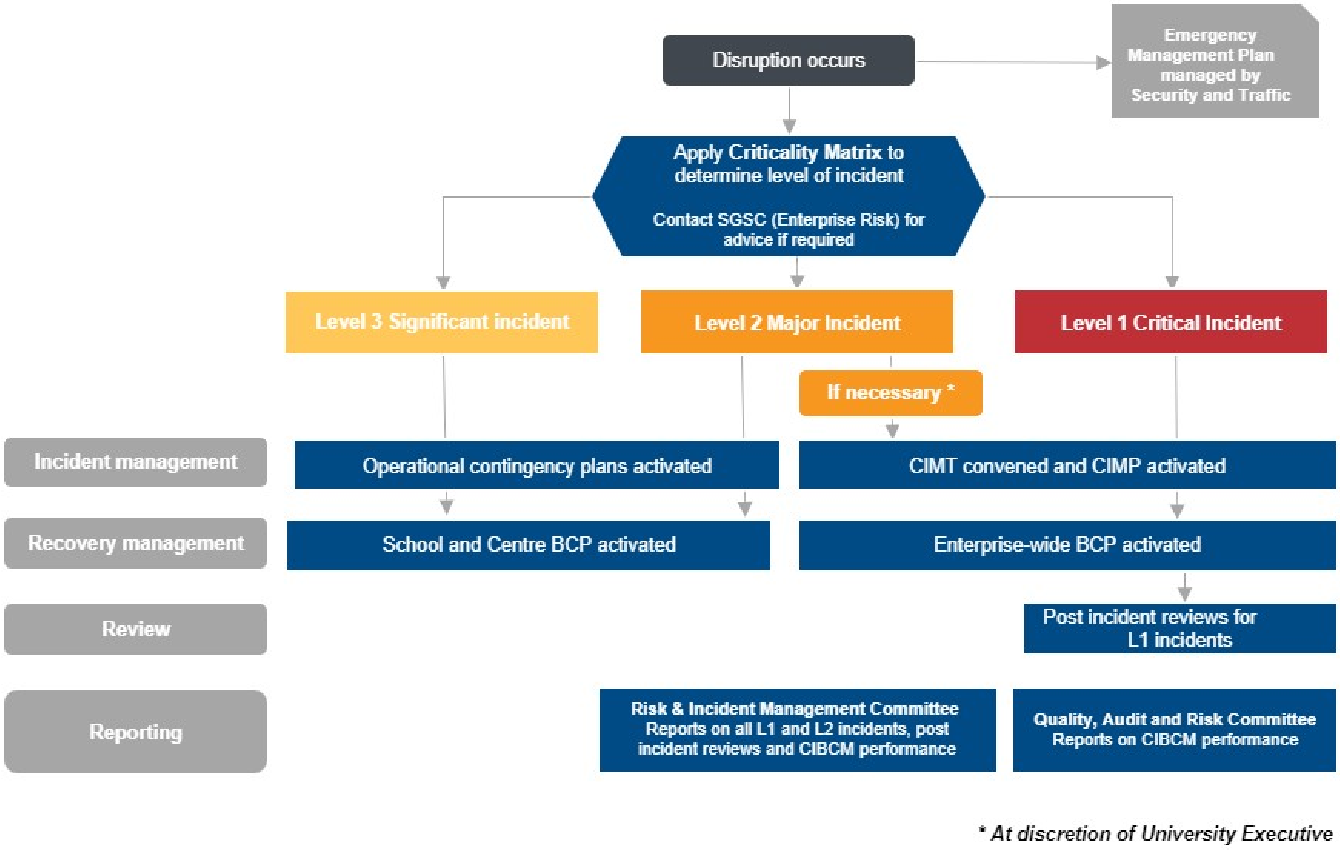
A critical incident is an event that poses a significant risk to the continuity of core University-wide operations. This level of incident may also have implications at the local, state, or national level.

Incidents occurring at ECU will vary and any impact will depend upon the geographical location, the potential to cause harm to people and the environment, and any economic or reputational impact upon the University.

Business continuity management is the system to prepare for, provide and maintain controls and capabilities for managing the University's overall ability to continue to operate during a major or critical incident.

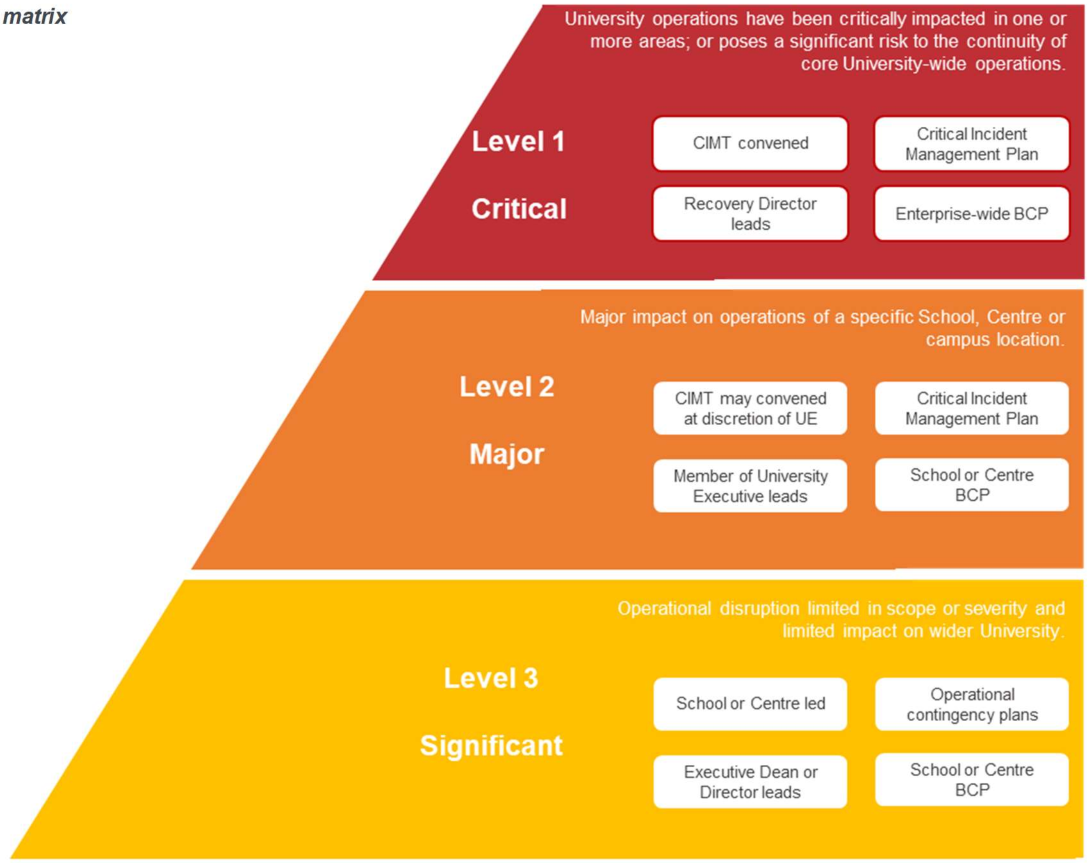
The flow from incident to recovery is illustrated in Figure 2 below:

Figure 2: Incident and recovery management flow


Disruption occurs
Emergency Management Plan managed by Security and Traffic
Apply Criticality Matrix to determine level of incident
Contact SGSC (Enterprise Risk) for advice if required
Level 3 Significant incident
Level 2 Major Incident
Level 1 Critical Incident
If necessary *
Incident management
Operational contingency plans activated
CIMT convened and CIMP activated
Recovery management
School and Centre BCP activated
Enterprise-wide BCP activated
Review
Post incident reviews for L1 incidents
Reporting
Risk & Incident Management Committee Reports on all L1 and L2 incidents, post incident reviews and CIBCM performance
Quality, Audit and Risk Committee Reports on CIBCM performance
* At discretion of University Executive

Incidents at ECU are categorised into one of three levels depending upon the level of support and resources required to manage the outcome. These category levels and incident criteria are detailed in the **Criticality Matrix** below:

Figure 3: Criticality matrix


University operations have been critically impacted in one or more areas; or poses a significant risk to the continuity of core University-wide operations.
Level 1
Critical
CIMT convened
Critical Incident Management Plan
Recovery Director leads
Enterprise-wide BCP
Major impact on operations of a specific School, Centre or campus location.
Level 2
Major
CIMT may convened at discretion of UE
Critical Incident Management Plan
Member of University Executive leads
School or Centre BCP
Operational disruption limited in scope or severity and limited impact on wider University.
Level 3
Significant
School or Centre led
Operational contingency plans
Executive Dean or Director leads
School or Centre BCP

3. Critical Incident Management Team (CIMT)

The Critical Incident Management Team is an incident specific team which is formed at the time a major or critical incident occurs and lasts until no longer required. As an executive group, the CIMT does not attend the incident scene. The CIMT will generally comprise of:

Role	Key responsibilities
Recovery Director *(Senior Deputy Vice-Chancellor or a relevant Deputy Vice-Chancellor)*	• Ensure effective management of the CIMT. • Ensure control of all organisational and operational implications. • Maintain communication flows with key stakeholders.
Human Resources Coordinator *(Director Human Resources Services Centre, or alternate, Manager Safety & Employment Relations)*	• Advice on human resources / people issues, including work health and safety. • Maintain appropriate staff counselling, welfare and recovery services and protocols.
Student Support Coordinator *(Director Student Life, or alternate, Manager Student Incident & Support)*	• Advice on student issues including student support needs. • Maintain all appropriate student counselling, welfare and recovery services and protocols.
Physical Resources Coordinator *(Director Digital and Campus Services, or alternate, Manager Campus Operations & Support)*	• Advice on physical resources / asset issues related to a crisis. • Work jointly with Human Resources Coordinator / Student Service Coordinator on any complementary crisis issues.
Information Technology Coordinator *(Chief Information Officer or alternate, Manager Information Security, Governance & Operations)*	• Support IT readiness for the crisis and support processes. • Manage IT recovery issues where required.
Communications Coordinator *(Manager Corporate Communications or alternate, Senior Communications Adviser*)	• Ensure that the communications strategy and protocols are ready to respond. • Provide advice on appropriate communication strategies to employ. • Coordinate all crisis-related internal and external communications. • Ensure adequate crisis media training for nominated spokespeople.
Governance and Compliance Coordinator *(Director Strategic and Governance Services or alternate, Manager Legal and Integrity)*	• Advice on legal, compliance, risk, regulatory, or academic governance matters. • Advice or reporting to external regulatory bodies.
CIMT Support Coordinator *(Chief Risk Officer or alternate, Senior Risk Adviser)*	• Ensure effective administrative support to CIMT. • Provide advice on enactment and content of Critical Incident Management Plan and/or Business Continuity Plans • Maintain communication flows with key stakeholders. • Organise CIMT meetings, document and record actions and follow-up.

At the time of the incident the CIMT may be expanded to include representatives of internal business units (Schools and Centres), or external agencies such as Department of Fire and Emergency Services (DFES) or Western Australia Police (WAPOL).

4. Incident communications

Timely, accurate and targeted delivery of communications during a disruption is key to ensuring an incident is managed and controlled appropriately.

For Critical Incidents (L1), it may be necessary for a Crisis Communications subgroup of the CIMT to be convened remotely after the CIMT, to discuss communication requirements in further detail.

The Crisis Communications subgroup will:

- Provide advice to the CIMT with regards to an appropriate media response and communication strategy.
- Ensure the crisis communication principles are adhered to.
- Provide feedback on the style and content of official university communications, including key messages, staff communications and media statements.
- Support the relevant business areas with advice on appropriate dissemination of key messages.

The Crisis Communications subgroup would typically comprise of:

- CIMT Recovery Director
- Vice-President (Enterprise & Development)
- Corporate Relations Manager
- Senior Deputy Vice-Chancellor
- Deputy Vice-Chancellor (Education), or alternate, Director Student Life
- Director Human Resources Services Centre, or alternate, Manager Safety & Employment Relations

The Critical Incident Management Plan contains further information to support crisis communications, including:

- Initial contact and escalation to involve the Corporate Communications team.
- Crisis communication principles, to be adhered to for all crisis communications.
- Approved crisis communication channels.

5. Post-incident reporting

Following a critical incident, a post incident review is to be conducted by the Strategic and Governance Services Centre (Enterprise Risk). A major incident may be subject to a post incident review if it is deemed that there are benefits from identifying lessons learnt that may be applicable to the wider University.

The review is to be completed within a reasonable timeframe following the end of a major or critical incident and the post incident report should be submitted to the Recovery Director and the Risk and Incident Management Committee.

6. Business continuity process

The business continuity process adopted by the University reflects the principles of international standard on business continuity, ISO22301:2019 *Security and resilience – business continuity management systems,* as set out in the figure 4.

Further guidance on the business continuity management process is provided overleaf.

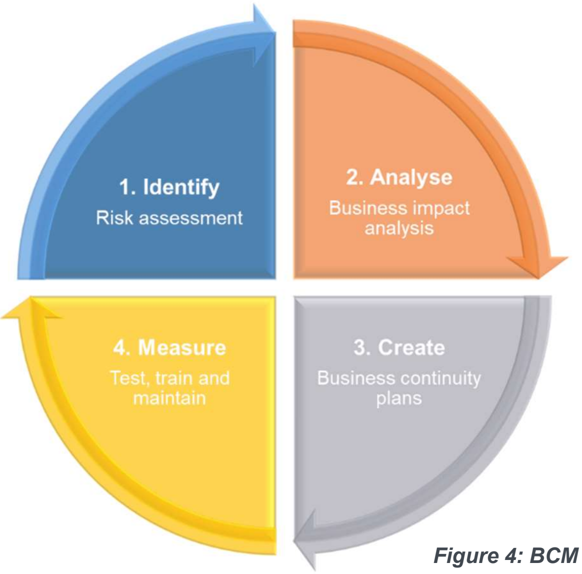


Figure 4: BCM cycle

Step	**1 – Identify** Risk Assessment	**2 – Analyse** Business Impact Analysis (BIA)	**3 – Create** Business Continuity Plans (BCP)	**4 – Measure** Test, train, maintain
Objective	To identify, analyse and evaluate the risk and assign a risk rating.	To measure the level of impact to organisational activities.	To create a BCP for a relevant area of the University, relevant to organisational requirements.	To test the effectiveness of the overall Business Continuity Management framework.
Description	The risk is described in terms of what could go wrong, in other words, the uncertainty of achieving the objectives. The risk identified must be relevant to the subject matter, appropriate given the context and useful for decision-making. Risk analysis involves determining the causes and consequences; as well as the existing controls that are in place to mitigate the risk. The risk is then evaluated by determining the likelihood of the risk occurring and the consequence if it does occur, by applying ECU's risk matrix. The result is a current or inherent risk rating.	The BIA is a systematic process to determine and evaluate the potential effects of an interruption to critical business operations. It prioritises business activities for recovery and identifies the resources that are required. The BIA attempts to answer: • What the impacts (consequences) are of a disruption. • What point in time the impacts become intolerable (unacceptable); and • What the dependencies and minimum resources requirements are for recovery.	A BCP is a document that details the actions that the School/Centre/University will take to continue operating during an unplanned disruption. The plan ensures that personnel and assets are protected and can function quickly in the event of a disruption. Each School and Centre is required to have a current, usable and available BCP using the BCP Template. BCPs are owned by the Centre Director for Centres, or Operations Manager for Schools. Enterprise Risk is responsible for the Enterprise-wide BCP.	This step ensures that what has been developed and documented will work when a crisis arises. Relevant employees are required to be trained in the use of the relevant plan. Enterprise Risk is responsible for running exercises to validate the completeness and accuracy of the University's plans.
Reference documents	Integrated Risk Management Guidelines	BIA Template	BCP Template	Enterprise Risk training schedule

7. Accountabilities and responsibilities

The following accountabilities and responsibilities apply with regards to critical incident and business continuity management at ECU:

- The University has responsibility to provide support in the strategic direction of recovery, including resources and infrastructure, during a business interruption.
- The Critical Incident Management Team (CIMT) has responsibility to provide leadership and control in the overall co-ordination, decision-making and communication strategies during an incident. They are also responsible for notifying areas to activate their Business Continuity Plans. Further information on the CIMT, including the role and details responsibilities can be found in Section 3.
- Each School and Centre has responsibility for the development, communication and ongoing maintenance of their Business Continuity Plan. Business Continuity Plans are to be reviewed at least annually by the relevant area representative.
- The Risk and Incident Management Committee (RIMC) has strategic oversight of incidents across the University and aims to reduce the overall risk associated with incidents, by reducing the impact of incidents which have occurred and the likelihood of reoccurrence.
- The Strategic and Governance Services Centre (Enterprise Risk) (SGSC) supports the RIMC and CIMT in incident management and provides specialist business continuity advice and is responsible for ensuring that the business continuity management process is implemented across the University and effective oversight is maintained through regular reporting and testing.